This Information Governance Framework should be read in conjunction with, but not exclusively with, the following:

- Information Governance Strategy and Policy;
- Records Management Policy;
- Data Protection Policy;
- Freedom of Information Policy;
- Personal File Guidance;
- ICT Security Policy;
- Communications Strategy;
- Consultation Strategy;
- Media Strategy;
- Social Media Policy;
- Discipline Policy & Procedure;
- Publication Scheme;
- Staff Code of Conduct; and
- Code of Conduct and Code of Accountability for NIFRS Board Members (*NB: to be formally adopted by Board*).

Relevant documents above will be reviewed in line with the requirements of the Information Governance Framework Strategy & Policy.
1 INTRODUCTION

This Information Governance Framework document sets out the approach to Information Governance in NIFRS.

As a general principle NIFRS information will be open, transparent and in the public domain, except where access or use of information is restricted for legislative reasons.

Having accurate, relevant and accessible information is vital to the efficient management of NIFRS, which values information as an important corporate asset.

NIFRS must, however, balance its aim to be open in its provision of information to the public and stakeholders, on which much confidence and trust is founded, with its obligations and duties around confidentiality and data protection.

NIFRS is required to create and manage all records efficiently, to make them accessible when needed, to protect and store them securely and to dispose of them safely at the appropriate time.

Effective information management benefits NIFRS by facilitating and supporting more efficient working, better decision-making, improved customer service and business transformation.

Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

NIFRS will deliver its Information Governance requirements in line with the HSC Information Management Controls Assurance Standard and will carry out annual self-assessments of its compliance against the criterion to determine whether their information is managed correctly. The requirement of the Information Management Controls Assurance Standard covers all aspects of Information Governance, including:

- Information Governance Management Framework;
- Information Risk Policy and Information Risk Management Strategy;
- Management of Corporate Records;
- Freedom of Information Act 2000;
- Personal Information;
- Information Governance awareness and training;
- Confidentiality and Data Protection skills, knowledge and experience;
- Information quality;
- Contractual arrangements;
- Information Life Cycle Management Strategy; and
- Individual requests for access to personal data.

There are many different statutory requirements and Standards that apply to Information Governance and information handling, including:
- Data Protection Act 1998;
- Freedom of Information Act 2000;
- Environmental Information Regulations 2004; and
- Good Management Good Records (GMGR) - guide to the required standards of practice in the management of records.

Non-compliance with this Framework and/or abuse of any electronic information, ICT resources or breach of any associated NIFRS policies may result in disciplinary action under the auspices of the Discipline Policy & Procedure.

2 STRATEGIC AIM

The aim of this Framework is to set out how NIFRS will effectively manage Information Governance. The organisation will achieve compliance by:

- Establishing robust Information Governance processes that conform to the HSC Controls Assurance Standard and comply with current legislation.

- Establishing, implementing and maintaining policies for the effective management of information.

- Ensuring that clear information is provided to staff and service users on how their personal information is recorded, handled, stored and shared.

- Providing clear advice and guidance to staff to ensure that they understand and apply the principles of Information Governance to their working practice.

- Sustaining an Information Governance culture through increasing awareness and promoting Information Governance, thus minimising the risk of breaches of personal data.

- Assessing NIFRS performance using the HSC Controls Assurance Standard self-assessment process and developing and implementing improvement plans to ensure continued improvement.

3 PURPOSE, VALUES AND PRINCIPLES

This document utilises and unifies existing and revised systems to create an integrated, co-ordinated, lean and sustainable Information Governance platform to support the aims of NIFRS and ensure information related legislative compliance.

This Framework is founded upon a number of Information Governance values and principles which will facilitate various key objectives. These in turn support the values and priorities of the organisation.
VALUES

<table>
<thead>
<tr>
<th>Openness and Transparency</th>
<th>Compliance and Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Making information more available to benefit the whole community.</td>
<td>Adhering to the appropriate legislative requirements to minimise the risk to public information through inappropriate use, unauthorised access or misuse.</td>
</tr>
</tbody>
</table>

PRINCIPLES

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Accessibility</th>
<th>Authenticity</th>
<th>Reliability</th>
<th>Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confining access to those with specific authority to view it.</td>
<td>Safeguarding the accuracy and completeness of information and ensuring the correct operation of all systems, assets and networks.</td>
<td>Ensuring that information is available and delivered to the right person, at the right time.</td>
<td>Ensuring that information and records are credible and authoritative.</td>
<td>Ensuring information and records can be trusted as a full and accurate representation of the transactions, activities or facts.</td>
<td>Ensuring there is an appropriate management framework in place to effectively implement information governance policies, programmes, protocols and guidelines.</td>
</tr>
</tbody>
</table>

The implementation of, and continued adherence to, this Framework and associated policies will be supported by an awareness raising and training programme.

4 SCOPE

This Framework document applies to all staff of NIFRS, including temporary and agency workers, who provide a service for NIFRS.

The information referred to in this document applies, but is not limited to information:

- stored on computers;
- transmitted across networks;
- printed out and/or filed in some form;
- written on paper and/or filed in some form;
- sent by fax;
- stored on tapes or disks;
- sent via email;
- stored on databases; and
- held on microfiche.

5 ROLES AND RESPONSIBILITIES

5.1 NIFRS Board

Overall responsibility for the efficient administration of the Information Governance lies with the Board.
5.2 Audit, Risk & Governance Committee

This Board Committee receives progress reports on the implementation of the Policy and Data Quality issues and will report to the Board accordingly. This Committee will appoint a suitable Information Governance Champion.

5.3 Accounting Officer

The Accounting Officer has overall responsibility for Information Governance within NIFRS. He/She is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Information Governance provides a framework to ensure information is used appropriately and is held securely.

5.4 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) has overall corporate responsibility for the Information Governance Framework/Strategy/Policy including Data Quality, FOI, Data Protection and Records Management.

Any breaches of the principles of this Framework should be reported to the Senior Information Risk Owner (SIRO) via SIRO@nifrs.org. Data errors should be reported through normal channels. Failure to comply with the Principles and Values within this Framework may result in disciplinary action under the auspices of the Discipline Policy & Procedure.

5.5 Personal Data Guardian

The Personal Data Guardian is the responsible officer for the purpose and manner in which personal data is collected, processed, stored, shared and dispensed with.

5.6 Directors and Heads of Departments

Day-to-day responsibility for administration and compliance with the Framework/Strategy/Policy is delegated from the Board through the Accounting Officer to respective Directors/Heads of Departments for their service area.

5.7 Information Management & Governance Group

The Information Management & Governance Group, made up of individuals that are suitably senior and/or with necessary expertise, will be delegated with the responsibility for the implementation and monitoring of Information Governance across the organisation. The work undertaken will be in line with the Group’s Terms of Reference as detailed at Appendix 1. The Group will report to the Senior Information Risk Owner (SIRO).
5.8 **Information Asset Owners (IAOs)**

The Information Asset Owners (IAOs) are responsible to their Head of Department or Director for liaison with the Information Management & Governance Group on all matters concerning administration of the Framework/Strategy/Policy:

- To work with the Director or Head of Department to ensure compliance in respect to systems within the Directorate.

- To work with the Director or Head of Department to ensure awareness of the need for Information Governance within the organisation, and to ensure that the control and handling of information within the Department or Station does not contravene any appropriate legislation or NIFRS procedures.

- To ensure that Data Quality requirements are included in all information systems.

5.9 **Managers**

Managers are responsible for ensuring that staff under their direction and control are aware of the policies, procedures and guidance laid down by the Senior Information Risk Owner (SIRO) through the Information Management & Governance Group and for checking that those staff understand and appropriately apply policies, procedures and guidance in respect of information governance in carrying out their day-to-day work.

5.10 **All Staff**

It is the responsibility of all staff to process information in accordance with the Data Protection Act 1998 and to adhere to the policies, procedures and guidance that are laid down by NIFRS for Information Governance and Security.

6 **REVIEW**

The Information Governance Framework will be reviewed annually, or as and when changes occur legislatively or within NIFRS.
APPENDIX 1

INFORMATION MANAGEMENT & GOVERNANCE GROUP
TERMS OF REFERENCE

1 Purpose

The purpose of this Group is to provide advice and assurance to the Director of Planning, Performance & Governance on all matters concerning Information Governance.

2 Definition

Information Governance is a framework to bring together all of the requirements, standards and best practice that apply to the handling of information. It allows organisations and individuals to ensure that information is accurate, dealt with legally, securely, efficiently and in order to deliver the best possible service. The principles of Information Governance, which is an organisational wide initiative, provide a consistent way for employees to deal with many different information handling requirements.

3 Outcome

NIFRS must achieve HSC Controls Assurance Compliance at the levels mandated and be able to evidence same.

4 Objectives

4.1 To ensure that NIFRS has effective policies and management arrangements covering all aspects of Information Governance in line with the organisation’s overarching Information Governance Policy, ie:

- Management of Information Governance;
- Information Security (including confidentiality, integrity and availability);
- Information Compliance (eg, Data Protection Act);
- Information Quality Assurance;
- Records Management; and
- Information Sharing.

4.2 To ensure compliance with Information Governance requirements placed on the organisation, particularly by the Information Governance Framework, to develop action plans where compliance is less than 100% and monitor their implementation.

4.3 To ensure that NIFRS undertakes or commissions annual assessments and audits of its Information Governance policies and arrangements.
4.4 To establish annual Information Governance Framework Improvement Plans, secure the necessary implementation resources and monitor the implementation of those plans.

4.5 To receive and consider reports into breaches of confidentiality and security and, where appropriate, undertake or recommend remedial action.

4.6 To ensure all relevant risks are recorded on the Corporate Risk Register.

4.7 To report to the Audit, Risk & Governance Committee, CMT and other working groups in order to promote Information Governance issues.

4.8 To ensure full and effective liaison with all external organisations, such as the Information Commissioner, local authorities and other relevant organisations.

4.9 To formulate and receive guidance from such supporting committees or groups as appropriate.

4.10 To report to the Corporate Management Team on Information Governance issues and to carry out such other tasks as may be required of it by the Director of Planning, Performance & Governance.

4.11 To identify where new policies and procedures are required or are in process of implementation and to assign responsibility for overseeing implementation of each policy and procedure.

5 **Accountability**

The Group reports to the Director of Planning, Performance & Governance who is the Senior Responsible Officer for Information Governance.

6 **Membership**

The Group membership will consist of nominated uniform and support personnel, staff with appropriate specialist roles and a Project Manager.

7 **Meetings and Reporting**

The Group will meet as often as necessary. Minutes of each meeting will be circulated within one week of the meeting.

8 **Approval and Review**

In line with these Terms of Reference, an Information Management & Governance Working Group has been established to deliver initial information project requirements.

The management of this going forward is yet to be determined.